PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06F 1/00, H04M 11/06 — A1

(11) International Publication Number: WO 91/05302

(43) International Publication Date: 18 April 1991 (18.04.91)

(21) International Application Number: PCT/GB90/01521

(22) International Filing Date: 4 October 1990 (04.10.90)

(30) Priority data:
8922473.7 5 October 1989 (05.10.89) GB

(71) Applicant *(for all designated States except US)*: AVANT GUARDIAN LIMITED [GB/GB]; 36 Grove Road, Sutton, Surrey SM1 1BS (GB).

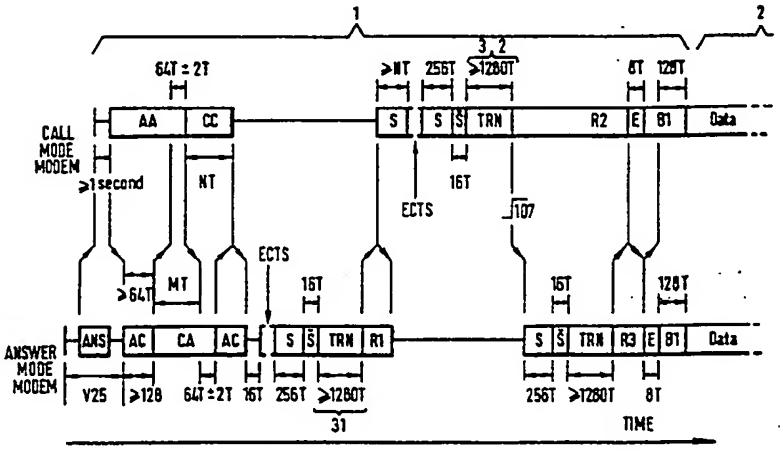
(72) Inventors; and
(75) Inventors/Applicants *(for US only)* : MACKENZIE, John, Richard, Stuart [GB/GB]; COLLINS, Bernard, Philip [GB/GB]; 36 Grove Road, Sutton, Surrey SM1 1BS (GB).

(74) Agent: PRICE, Paul, Anthony, King; D. Young & Co., 10 Staple Inn, London WC1V 7RD (GB).

(81) Designated States: AT, AT (European patent), AU, BB, BE (European patent), BF (OAPI patent), BG, BJ (OAPI patent), BR, CA, CF (OAPI patent), CG (OAPI patent), CH, CH (European patent), CM (OAPI patent), DE, DE (European patent), DK, DK (European patent), ES, ES (European patent), FI, FR (European patent), GA (OAPI patent), GB, GB (European patent), HU, IT (European patent), JP, KP, KR, LK, LU, LU (European patent), MC, MG, ML (OAPI patent), MR (OAPI patent), MW, NL, NL (European patent), NO, RO, SD, SE, SE (European patent), SN (OAPI patent), SU, TD (OAPI patent), TG (OAPI patent), US.

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A METHOD OF CONTROLLING ACCESS TO RESTRICTED ACCESS DATA AND COMMUNICATION SYSTEM THEREFOR



(57) Abstract

In electronic communication systems, negotiations are performed between two pieces of apparatus (e.g. modems) in order to ensure technical compatibility during subsequent data transmission. Instead of performing security checks in the known manner after the negotiations have been completed (e.g. sending an access code or identity code), the invention teaches that the negotiations themselves should be customized to include security checks. For example, during negotiations between a call modem and an answer modem, the call modem includes a "first indication" in the negotiations. The answer modem detects the "first indication" and permits the call modem to have access to restricted access data during data transmission after the negotiations have been completed. The "first indication" may comprise a negotiation segment having a precise length and/or containing an embedded code. The answer modem may include a "second indication" in the negotiations in order to trigger the call modem to produce the "first indication". Also, the call modem may include a "third indication" in the negotiations after the "first indication" in order to identify more precisely or uniquely the call modem.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MC	Monaco
AU	Australia	FI	Finland	MG	Madagascar
BB	Barbados	FR	France	ML	Mali
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Fasso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GR	Greece	NL	Netherlands
BJ	Benin	HU	Hungary	NO	Norway
BR	Brazil	IT	Italy	PL	Poland
CA	Canada	JP	Japan	RO	Romania
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SN	Senegal
CM	Cameroon	LI	Liechtenstein	SU	Soviet Union
DE	Germany	LK	Sri Lanka	TD	Chad
DK	Denmark	LU	Luxembourg	TG	Togo
				US	United States of America

A METHOD OF CONTROLLING ACCESS TO RESTRICTED ACCESS DATA AND COMMUNICATION SYSTEM THEREFOR

This invention relates to the controlling of access to restricted access data.

With the ever growing use of electronic communication systems, it is necessary to ensure that only authorised users obtain access to restricted access data. For example, a computer may be accessible via the public telephone network by having a modem that links up, via the telephone network, with the modem of a user. Normally, the decision as to whether to permit access to any restricted access data in the computer is determined by whether the user transmits, via the modems, an approved access code or identity code to the computer. However, so-called "hackers" are able by detailed knowledge of existing systems or by persistent guessing of possible identity codes to gain access to restricted access data in computers.

Accordingly, there is the need for an arrangement in which the "hacker" is unaware that he is being vetted as to whether or not he is entitled to access to the restricted access data. Alternatively, if the "hacker" is aware that he is being vetted, he must be unable to work out how to circumvent the security features.

According to a first aspect of the present invention, a method of enabling a first apparatus to determine whether or not a second apparatus should be permitted access to restricted access data comprises the steps of:

the first and second apparatuses performing joint negotiations to ensure technical compatibility for data transmission between themselves;

the first apparatus monitoring the negotiations to detect whether, within the negotiations, there is a first indication originating from the second apparatus that the first apparatus recognises as indicating that the second apparatus is entitled to access to the restricted access data; and

the first apparatus responding if it detects the first indication, whereby the response of the first apparatus may be used to permit the second apparatus to gain access to the restricted access data when data transmission starts after the negotiations have been completed.

If, for example, the first and second apparatuses are answer and call modems respectively, then the negotiations may be the start-up procedure that modems automatically perform without any active participation by the user whose personal computer, for example, is connected to the call modem. Because the user is vetted automatically during the start-up procedure, the user is not aware that his security status is being checked. Start-up procedure negotiations are illustrated in Figure 4/V.32 of the CCITT Recommendation V.32 relating to "A family of 2-wire, duplex modems operating at data signalling rates of up to 9600 bit/s for use on the general switched telephone network and on leased telephone-type circuits". Whilst some of the start-up procedure is precisely determined by the V.32 Recommendation, there are certain parts of the procedure where the exact format of the signals is not precisely laid down. It is during such parts of the procedure that the first indication may be included in the start-up negotiations.

Because the first indication may be included within existing standard modem procedures, such as the start-up procedure, the present invention may be made compatible with existing modem arrangements.

As it is possible that the first indication might be included in the negotiations by the second apparatus purely by chance, it is preferable that the method further includes the steps of:

the first apparatus including a second indication in the negotiations;

the second apparatus monitoring the negotiations to detect whether, within the negotiations, there is the second indication; and

the second apparatus including the first indication in the negotiations only if the second apparatus has already detected the second indication.

Because the first indication is generated in response to the second indication, it is less likely that the second indication will be included in the negotiations purely by chance compared with the arrangement where the first apparatus merely monitors for the presence of the first indication without having triggered the generation of the first indication

by itself producing the second indication. Thus, an extra element of security is included.

It is envisaged that the first indication may, for example, identify the second apparatus as belonging to a group of apparatuses which are permitted access to the restricted access data. For example, the second indication may inform the first apparatus that the second apparatus is an authorised piece of apparatus belonging to company X. However, the first apparatus does not know exactly which of the possibly many authorised pieces of apparatuses belonging to company X the particular second apparatus it is communicating with happens to be. Thus, it is preferable that the method further includes the step of the second apparatus including a third indication in the negotiations after it has included the first indication in the negotiations. The third indication may therefore be used to identify more precisely or even uniquely the second apparatus. For example, the third indication could identify the second apparatus as being the piece of apparatus in the Accounts Department within company X. This gives an extra piece of knowledge to the first apparatus which was previously only aware, by virtue of the first indication, that the second apparatus was one of the many authorised apparatuses belonging to company X.

According to a second aspect of the present invention, a communication system comprises:

a first apparatus for controlling access to restricted access data; and

a second apparatus;

the first and second apparatuses including respective means for performing joint negotiations to ensure technical compatibility for data transmission between the first and second apparatuses;

the second apparatus further including means for including in the negotiations a first indication indicating that the second apparatus is entitled to access to the restricted access data; and

the first apparatus further including means for monitoring the negotiations to detect the first indication and means for responding to the detection of the first indication, whereby the response of the first

apparatus may be used to permit the second apparatus to gain access to the restricted access data when data tranmission starts after the negotiations have been completed.

Preferably, the first apparatus further includes means for including in the negotiations a second indication, and the second apparatus further includes means for monitoring the negotiations to detect the second indication and means for activating the first indication inclusion means in response to the detection of the second indication.

Preferably, the second apparatus further includes means for including in the negotiations a third indication after the first indication.

The invention will now be described by way of non-limiting example with reference to the accompanying drawings in which:-

Figure 1 is a diagram illustrating a 16-point signal structure with non-redundant coding for 9600 bit/s and subset A,B,C,D of states used at 4800 bit/s and for training; and

Figure 2 is a diagram illustrating the start-up procedure negotiations between modems prior to the transmission of data between the modems.

Figures 1 and 2 describe an example of the invention in the context of modem to modem communications as described in CCITT Recommendation V.32. A full explanation regarding signal states A,B,C,D as shown in Figure 1 is given in section 2.4 of Recommendation V.32.

Also a full explanation regarding the start-up procedure negotiations is given in section 5 ("Operating Procedures") of Recommendation V.32.

Referral should be made to Recommendation V.32 in order to achieve a full understanding of the known start-up procedure specification.

However, in order to assist understanding of Figure 2, there is reproduced below a table identifying the nature of the individual segments identified in Figure 2.

ANS	Answer tone in accordance with CCITT Recommendation V.25.
AC	Signal states ACAC..AC for an even number of symbol intervals T; similarly with CA,AA and CC.
MT,NT	Round-trip delays observed from answer and call modems respectively, including 64T±2T modem turn round delay.
S,$\overline{S}$	Signal states ABAB..AB, CDCD..CD.
TRN	Scrambled ones at 4800 bit/s with dibits encoded directly to states A, B, C and D as defined in section 5.2, c) of CCITT Recommendation V.32.
R1, R2, R3	Each a repeated 16-bit rate sequence at 4800 bit/s scrambled and differentially encoded as in Table 1 of CCITT Recommendation V.32.
E	A single 16-bit sequence marking and following the end of a whole number of 16-bit rate sequences in R2 and R3.
B1	Binary ones scrambled and encoded as for the subsequent transmission of data.
ECTS	Optional special echo canceller training sequence.

This example of the present invention relies on the fact that Recommendation V.32 does not specify precisely all features of the negotiations labelled 1 in Figure 2 that occur prior to data transmission 2. The negotiations 1 comprise the start-up procedure between the call and answer modems.

The negotiations 1 include segments 31 and 32 of a type called TRN which serve to train the adaptive equaliser in the receiving modem and the echo canceller in the transmitting modem. As may be seen from Figure 2, recommendation V.32 specifies that the TRN segments must be greater than or equal to 1280 symbol intervals T. A symbol interval T is the interval associated with one of the signal states A,B,C or D as shown in Figure 1. Also, Recommendation V.32 only specifies the nature of the first 256 symbols. There is therefore leeway as to exactly which symbols are selected to be the 257th symbol onwards and exactly how many symbols there should be, subject to the requirement that the total number of symbols associated with segment TRN is greater than or equal to 1280.

Thus, an indication may be given by choosing the total number of symbols to be a precise number, for example, 2036 symbols.

Thus, TRN segment 32 may be carefully arranged to provide the "first indication" of the present invention. TRN segment 32 has to be present in accordance with Recommendation V.32 but it is by choosing its parameters within the possibilities allowed by the Recommendation that it may be made to serve the purpose of the "first indication". This may be done by, as mentioned above, arranging for TRN segment 32 to have a precise symbol length. Alternatively, because the symbols from the 257th symbol onwards are unspecified, it may be arranged that within the TRN segment 32, after the 257th symbol, there is a predetermined code of the symbols A,B,C,D which the answer modem identifies as being the "first indication". Such a predetermined code of symbols may be likened to a gene contained within a chromosome.

Including such a code in TRN segment 32 will require the scrambler in the call modem to be returned to a known condition consistent with the state of the descrambler in the answer modem. Scrambler/descramblers are discussed in section 4 of Recommendation V.32.

Prior to the "first indication" being included in the start-up procedure negotiations by the call modem by customizing the characteristics of the TRN segment 32, the answer modem produces its own customized TRN segment 31, which serves as a "second indication".

The call modem monitors for the presence of the customized TRN segment 31 and only produces its own customized TRN segment 32 if it detects the presence of customized TRN segment 31. If the TRN segment 31 is not correctly customized (i.e. no "second indication" is present), then the call modem will produce a TRN segment 32 that does not contain the "first indication", e.g. by giving the segment a length of 2500 symbols or ensuring that it does not contain the predetermined code of the symbols A,B,C,D.

The customized TRN segment 31 may therefore be likened to a "nod" that is produced by the answer modem and which triggers off the production of a "wink" by the call modem in the form of the customized TRN segment 32.

The customized TRN segment 32 may in practice be capable of being produced by a large number of modems and thus, when the answer modem receives the customized TRN segment 32, it is unable to identify precisely which modem it is connected to.

Therefore, the call modem produces a "third indication" that is used to identify precisely which modem it is. The "third indication" is produced by the call modem after it has produced the "first indication". If the "first indication" is in the form of a predetermined code of signal states A,B,C,D embedded within TRN segment 32, then the "third indication" may also comprise a predetermined code of signal states A,B,C,D appearing in the TRN segment 32, but after the "first indication".

In the context of modems, it is envisaged that the present invention may be implemented by modifying standard modems that are in accordance with Recommendation V.32. These modems, because they remain in accordance with Recommendation V.32, are capable of working normally without providing a security checking function. However, in order to achieve such a security function, the modems will contain additional circuitry over and above that required to satisfy Recommendation V.32 so as to to provide the first, second and third

indications and to respond thereto. Thus, additional circuitry in the answer modem will, upon detecting the first indication, produce a response (e.g. a signal) which permits the data transmission 2 subsequent to the start-up procedure negotiations 1 to involve the restricted access data. In simple terms, the signal produced by the answer modem may, for example, activate a switch so that a computer database accessed via the answer modem permits the, for example, personal computer connected to the call modem to have access only to non-restricted data if the signal produced in response to the first indication is not present, but to have access to the restricted access data if the signal produced in response to the first indication is present.

It is to be understood that the present invention is not restricted to implementation in the context of modems. For example, a pair of computers might be connected by dedicated telephone lines and it is desirable that, every time they communicate with one another, they check that they are indeed authorised to pass restricted access data between themselves. Thus, there may be hardware or software within the computers which, during the negotiations involved prior to data transmission, effect the incorporation and detection of at least the first indication in the negotations in order to ensure security.

The third indication, instead of being included within the TRN segment 32, could, for example, be incorporated within additional negotiations which are not shown in Figure 2. For example, after the start-up procedure negotiations 1, there could be additional negotiations associated with error correction and/or data compression which occur after the start-up procedure negotiations 1 but before data transmission 2. The third indication could therefore be incorporated in the error correction and/or data compression negotiations.

CLAIMS

1. A method of enabling a first apparatus to determine whether or not a second apparatus should be permitted access to restricted access data comprising the steps of:

the first and second apparatuses performing joint negotiations to ensure technical compatibility for data transmission between themselves;

the first apparatus monitoring the negotiations to detect whether, within the negotiations, there is a first indication originating from the second apparatus that the first apparatus recognises as indicating that the second apparatus is entitled to access to the restricted access data; and

the first apparatus responding if it detects the first indication, whereby the response of the first apparatus may be used to permit the second apparatus to gain access to the restricted access data when data transmission starts after the negotiations have been completed.

2. A method according to claim 1, further including steps of:

the first apparatus including a second indication in the negotiations;

the second apparatus monitoring the negotiations to detect whether, within the negotiations, there is the second indication; and

the second apparatus including the first indication in the negotiations only if the second apparatus has already detected the second indication.

3. A method according to claim 1 or claim 2, further including the step of the second apparatus including a third indication in the negotiations after it has included the first indication in the negotiations.

4. A communication system comprising:

a first apparatus for controlling access to restricted access data; and

a second apparatus;

the first and second apparatuses including respective means for performing joint negotiations to ensure technical compatibility for data transmission between the first and second apparatuses;

the second apparatus further including means for including in the negotiations a first indication indicating that the second apparatus is entitled to access to the restricted access data; and

the first apparatus further including means for monitoring the negotiations to detect the first indication and means for responding to the detection of the first indication, whereby the response of the first apparatus may be used to permit the second apparatus to gain access to the restricted access data when data tranmission starts after the negotiations have been completed.

5. A communication system according to claim 4, wherein the first apparatus further includes means for including in the negotiations a second indication, and the second apparatus further includes means for monitoring the negotiations to detect the second indication and means for activating the first indication inclusion means in response to the detection of the second indication.

6. A communication system according to claim 4 or claim 5, wherein the second apparatus further includes means for including in the negotiations a third indication after the first indication.

1/1

FIG.1

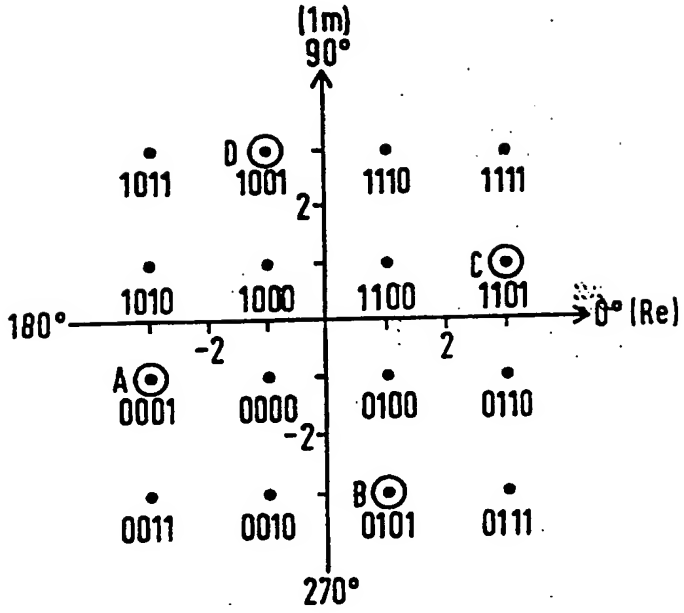
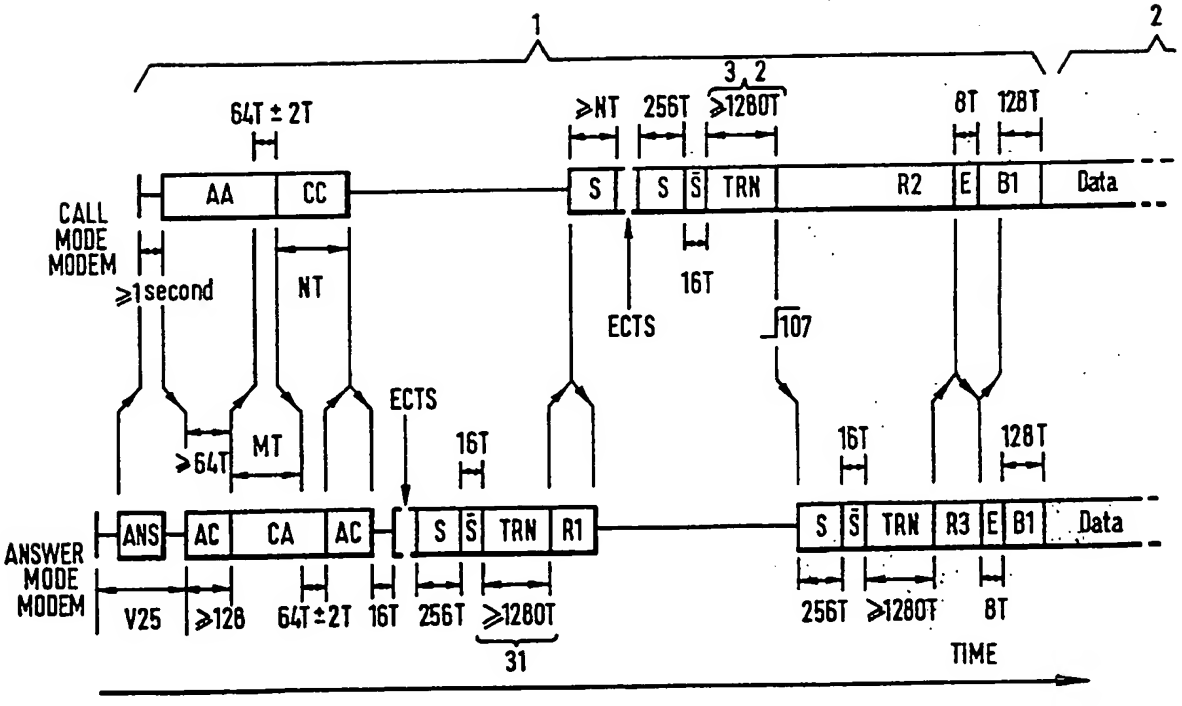


FIG.2 V



INTERNATIONAL SEARCH REPORT

International Application No PCT/GB 90/01521

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC[5]: G 06 F 1/00, H 04 M 11/06

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC[5]	G 06 F, H 04 M, H 04 L

Documentation Searched other than Minimum Documentation to the Extent that such Documents are included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
Y	Patent Abstracts of Japan, vol. 12, no. 138 (P-695)(2985), 27 April 1988, & JP, A, 62260260 (NEC CORP.) 12 November 1987 see abstract	1,4
Y	EP, A, 0292691 (HAYES) 30 November 1988 see claim 1	1,4
A		2,3,5,6
A	EP, A, 0258945 (PHILIPS') 9 March 1988 see page 5, lines 23-36	1,4

./.

* Special categories of cited documents: [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
28th December 1990	22.02.91
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	Alfredo Prein

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)		
Category *	Citation of Document, ** with indication, where appropriate, of the relevant passages	Relevant to Claim No.
A	EP, A, 0258716 (HAYES) 9 March 1988 see column 3, lines 21-56; column 12, lines 40-51	1,4

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO. GB 9001521 SA 40554

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 16/01/91 The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A- 0292691	30-11-88	US-A-	4894847	16-01-90
		AU-B-	598120	14-06-90
		AU-A-	1408388	01-12-88
		AU-A-	5120090	28-06-90
		AU-A-	5120190	28-06-90
		AU-A-	5120290	28-06-90
		JP-A-	63305645	13-12-88
EP-A- 0258945	09-03-88	NL-A-	8602245	05-04-88
		JP-A-	63064441	22-03-88
		US-A-	4922521	01-05-90
EP-A- 0258716	09-03-88	US-A-	4782498	01-11-88
		AU-B-	585168	08-06-89
		AU-A-	7681087	03-03-88
		CA-A-	1273689	04-09-90
		JP-A-	63132552	04-06-88